Performance Measures	Go	No-Go	N/A
Does the command's IA user training program comply with the Army minimum training requirements? IAW AR 25-2, Para. 4-3a(8); DoD 8570.1-M, Para. C6.2.5; DoDI 8500.2 IA Control PRTN			
Do all users complete initial IA Awareness training before receiving network access? IAW AR 25-2, Para. 4-3a(8)(a and b), NIST 800-53 Appendix F AT2, CJCSM 6510.01 Appendix B Enclosure A Para. 5 and Appendix A 2-3			
Do all users complete refresher IA Training annually? IAW AR 25-2, Para. 4-3a(8)(a and b), NIST 800-53 Appendix F AT2, CJCSM 6510.01 Appendix B Enclosure A Para. 5 and Appendix A Enclosure A Para. 7b, DoD 8570.1-M Para. C6.2.2; DODD 8570.1 5.9.2; DoDI 8500.2 IA Control PRTN			
Have all IA personnel in Technical Levels I-III completed the Army required minimum training within six months of appointment to the position? IAW AR 25-2, Para. 4-3a(2), (6)(a-c); DoD 8570.1-M C3.2.3.1; IA Training and Certification Best Business Practice, Para. 11f, g, and h; DoDI 8500.2 IA Control PRTN			
Have all IA personnel in Management Levels I-III completed the Army required minimum training within six months of appointment? IAW Army IA Training and Certification Best Business Practice, Para. 11a, b, and c			
Have all IA personnel in Management Levels I-III obtained the appropriate DoD IA baseline commercial certification within six months of appointment? IAW AR 25-2, Para. 4-3a(1)(d); DoD 8570.1-M C4.2.3.2, C9.3.2.5 C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Para. 11a, b, c			
Have all IA personnel in Technical Levels I-III obtained the appropriate DoD IA baseline commercial certification within six months of appointment? IAW AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1, C9.3.2.5, C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Para. 11 f, g, h			
Have all IA personnel in Technical Levels I-III obtained the appropriate computing environment certification, within six months of appointment? IAW AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1, C9.3.2.5, C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Para. 11 f, g, h			

Has the organization met the appropriate IAM and IAT certification milestones (100% by 31 Dec 2010)? IAW AR 25-2, Para. 4-3a(1)(d); DoD 8570.1-M C4.2.3.2, C9.3.2.5 C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Para. 11a, b, c			
Are all IAT/IAM/IASAE/CND-SP category personnel fully trained and certified to prior to deployment to a combat environment? IAW AR 25-2 4.3a(6)(a)&(d); DoD 8570.1-M C3.2.4.1.1, C9.3.2.5, C.4.2.3.2 and C.9.3.2.5.1-3; IA Training and Certification BBP, Para. 11 f, g, h			
Do all IT services contracts state the contractor personnel must obtain the appropriate baseline and computing environment certification(s)? IAW DOD 8570.1-M Para. C1.4.4.12, C7.3.4.4, C1.4.4.5, C2.1.5, C1.4.4.12,C3.2.4.8.1, C4.2.3.1; DFAR Section 239; IA Training and Certification BBP, Para. 1			
Is the Security Manager, IMO, SA, NM, and/or IASO identified in writing on orders? AR 25-1 C3-2.e.4; AR 25-2 C3-3			
Are the Security Manager, IMO, SA, NM, and/or IASO registered appropriately in ATCTS at their designated IT level?			
Is the IMO(s) aware of the site where the JBLM IA documents can be obtained?			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Does each Information System have a current Interim Authorization To Test (IATT), Interim Approval To Operate (IATO) or Approval To Operate (ATO) and/or an approved Tenant Security Plan? AR 25-2, Para. 5-8(b); Army Information Assurance Certification and Accreditation BBP, Para. 10.L; DoDI 8510.01, E3. Enclosure 3, The DIACAP Package			

Does the IMO/SA/IASO have a copy of the Certificate of Networthiness (CoN) for additional software loaded on workstations? AR 25-1 App. C			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Are miscellaneous processing equipment appropriately labeled (i.e. workstations, copiers, facsimile machines, peripherals, typewriters, word processing systems, etc.)? AR 25-2, Para. 4-17c(1-5); AR 380-5, Para 4-1 and 4-34a and b; DoDI 8500.2 IA Control ECML			
Are wired/wireless portable electronic devices (PEDs) prohibited from areas where classified information is discussed or electronically processed? AR 25-2, Para. 4-29a and 6-5 a.; DoDD 8100.2 Para. (4.2) (4.3) (4.4); DoDI 8500.2 IA Control ECWN			
Does the organization physically control and securely store information system media (paper and digital) based on the highest classification of information on the media to include pickup, receipt, transfer and delivery of such media to authorized personnel? AR 25-2, Para. 4-16(a and b), DoD 5200.1-R, c7.2.1.1.4, c7.2.1.1.5, c7.2.1.2, c7.2.2, ap7.4.1; DoDI 8500.2 IA Control PESS			
Does the organization sanitize or destroy classified information system digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using the information contained on the media? AR 25-2, Para. 4-18(b-j); AR 380-5, Para. 3-18; Reuse of Computer Hard Drives BBP; DoDI 8500.2 IA Control PECS			
Does the organization ensure only authorized maintenance personnel with a need-to-know are granted physical access to classified information systems? AR 25-2, Para. 4-10 (d), AR 380-5, Para. 6-1; DoDI 8500.2 IA Control PRMP			

Does the organization ensure all classified removable media (Thumb Drives, floppies, USB hard drives, CDs, etc.) and classified information systems comply with all requirements for marking and labeling? AR 25-2, Para. 4-17 (a-d); AR 380-5, Para. 4-33; DoD 5200.1-R, Para. C5.4.9 and C5.4.10; DoDI 8500.2 IA Control ECML			
Does the organization ensure devices that display or output classified information in human-readable form are positioned to deter unauthorized individuals from reading the information? DoDI 8500.2 IA Control PEDI			
Does the organization ensure only approved Keyboard, Video, and Mouse (KVM) switch boxes are in use for switching between systems of different classification levels? AR 25-2 Para. 4-20(h), KVM BBP; DoDI 8500.2 IA Control DCBP			
Is the classified network transmission protected with NSA Type 1 Cryptographic devices and/or a compliant and approved Protected Distribution System (PDS)? AR 25-2, Para. 6-3, NSTISSI 7003, and IA Control ETCT			
Is unattended classified information (to include IS media and keyed Controlled Cryptographic Items) stored in either a GSA Approved container or approved open storage area? AR 380-5 Para 7-4a; TB380-41 Para 5.3			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
DOCUMENTS			
Have all IASO, SA, IMO and/or Alternates been appointed in writing by the commander?			
Are appointment orders, AUP/PLAA, certifications, and training loaded in ATCTS? Does IMO have ASCL cards?			
Does primary IMO have TSP, applicable regulations, polices, and memorandums available?			
Is all data in the DIACAP listed correctly?			
USER ACCOUNTS			

Are all unit users registered in ATCTS?			
Are all users/user accounts/profiles listed under the unit correctly and the unit listed under 18th Airborne Corps			
Do all primary and alternate IMO's have a Remedy Account and receive Remedy emails			
INFORMATION SYSTEMS			
Are all systems imaged with the current AGM for Vista?			
For systems not Vista/AGM compliant, has an exemption been completed, signed, and submitted?			
Are all systems (network and travel) updated with the latest IAVAs?			
Are systems (classified/unclassified) marked with applicable labels?			
Are classified systems stored correctly?			
Are systems up to date with virus definitions?			
Has a Data-At-Rest (DAR) solution been implemented/activated on all systems (network/standalone)			
How many and what types of servers are in your unit?			
Are local or generic accounts prohibited? Are system logs audits turned on?			
Are administrator and guest accounts renamed? Is the Guest account renamed and disabled?			
d. Are system administrator privileges restricted?			
STAMIS AND STANDALONE SYSTEMS			
Identify all STAMIS, Program of Record, Standalone systems.			
Does IMO/SA/IASO have a copy of the Certificate of Networthiness (CON) for additional software loaded on the machine?			
Are the IASO, IMO Server/Workstation Administrators and/or Alternates ensuring that STAMIS systems (any Logistic system) and standalone systems are being patched and updated as required?			
Does system require authentication for access (login/password)?			
Are all user/system passwords 15 characters long, with 2 upper, 2 lowercase letters, 2 numbers, and 2 special characters?			
Are systems up to date with IAVA patches and Antivirus definitions? How often are standalone systems are in the unit patched (SOP)?			
Are systems set to lock screen and activate screensaver after 10min?			
DOD INFORMATION ASSURANCE CERTIFICATION AND ACCREDITATION PROCESS (DIACAP)			
Are all systems recorded in the DIACAP?			

Is all data in the DIACAP listed correctly?			
Does your unit have a completed and approved Tenant Security Plan?			
Does primary IMO/SA/IASO have a copy of the approved TSP?			
EMERGENCY PLANNING			
Are written procedures (SOP) in place (risk management) outlining appropriate actions to take regarding classified and unclassified systems in case of emergency?			
Data At Rest (DAR)/Personal Identifiable Information (PII)			
Are all travel laptops marked as such and have the applicable DAR solution applied?			
Have all applicable DoD workstations/laptops compliant with an active DAR solution?			
Are PII documents being protected while at rest on the information system?			
Are Unit procedures for PII incidents prescribed?			
GENERAL INFORMATION			
Is there any wireless communications equipment being utilized in the unit?			
Are all IMOs able to access NEC IMO site?			
Is the Security Manager identified in writing on orders?			
Does the unit have an IAM? Are they registered in ATCTS as a manager?			
Does the unit have an IASO? Are they registered in ATCTS as a manager?			
Has additional software been added to any system above the current AGM load? Does the IMO or system owner have a CON for the software?			
Is the IMO(s) aware of the site where the FB IA documents can be obtained?			
Are system backup procedures identified in the unit's Standard Operating Procedures (SOP)? Are workstation files backed up regularly?			
Performance Measures	**Go**	**No-Go**	N/A
Are personnel required to sign a user agreement prior to being granted access to the information system? (This also includes privileged users signing a Privileged Access Agreement prior to receiving privileged access.) AR 25-2, Para. 3-3c(1), 4-3; ALARACT 158-2008, Section 2; BBP 06-PR-M-0003 (Privileged Access Agreement AUP), Para. 8; DoDI 8500.2 IA Control PRRB			

Are media that will be reused in an alternative Army environment purged with an approved Army or DoD wiping tool prior to release to the other Army organization? AR 25-2, Para. 4-18a, b, and d; BBP 03-PE-O-0002 (Reuse of Computer Hard Drives), Para. 7A(1); DoDI 8500.2 IA Control PECS			
Are media which stored classified or sensitive (to include restricted, test, research, or PII) information degaussed with an NSA-approved degausser and destroyed using an NSA-approved destruction method? AR 25-2, Para. 4-18a, e, and g; BBP 03-PE-O-0002 (Reuse of Computer Hard Drives), Para 7A(5)			
Are purged/destroyed media actions documented on a media disposition certification label AND in a Memorandum of Record (MoR)? AR 25-2, Para. 4-18a; BBP 03-PE-O-0002 (Reuse of Computer Hard Drives), Para. 9A(5), 9B(9), and 9C(7)			
Is the MoR retained for at least five years? AR 25-2, Para. 4-18a; BBP 03-PE-O-0002 (Reuse of Computer Hard Drives), Para. 9A(5), 9B(9), and 9C(7)			
Do authorized users who are contractors, DOD direct or indirect hires, foreign nationals, or foreign representatives have their respective affiliations incorporated as part of their e-mail addresses? AR 25-2 Para. 4-20f(8); ALARACT 021/2010; DoDD 8500.01E Para. 4.10; DoDI 8500.2 IA Control ECAD-1			
Do authorized users who are contractors, DOD direct or indirect hires, foreign nationals, or foreign representatives have their respective affiliations identified within their display names? AR 25-2, Para. 4-15a and 4-20f(8); DoDI 8500.2 IA Control ECAD1			

Do authorized users who are contractors, foreign nationals, or foreign representatives have their respective affiliations indicated in an automated signature block? AR 25-2, Para. 4-15c; DoDI 8500.2 IA Control ECAD1			
Do users meet the personnel security requirements for gaining access to Army information systems? AR 25-2 Para. 4-5c(3) and 4-14a; DoDI 8500.2 IA Control PRAS			
Has the appropriate authority formally appointed his/her IA workforce personnel (i.e. appointment orders)? AR 25-2 Para. 2-24f and Chapter 3			
Are contractor personnel positions designated as IT-I, IT-II, IT-III, or IT-IV for access to the IS? AR 25-2, Para. 4-14			
Are the background check requirements included in maintenance contracts, statements of work, and specified on the DD Form 254 (Department of Defense Contract Security Classification Specification)? DoDI 8500.2 IA Control PRAS-1 (Sensitive) or PRAS-2 (Classified); DFARS Section 239			
Are foreign exchange personnel and representatives of foreign nations (not to be confused with foreign nationals) limited to email only access, unless further access is vetted through the Army G-2 Foreign Disclosure and Security Directorate, and authorized by Army CIO/G-6? AR 25-2 Para. 4-15b and 4-15d; DoDD 8500.01E Para. 4.9			
Does the organization restrict the use of employee owned information systems (EOIS)? AR 25-2, Para. 4-31; AR 25-1, Para. 6-1i			

Does the organization ensure all removable media (to include, but not limited to Thumb Drives, floppies and CDs) and information systems comply with all requirements for marking and labeling contained in policy and guidance documents? AR 25-2, Para. 4-17 (a-d); AR 25-55, Para. 4-200d; DoDI 8500.2 IA Control ECML			
Does the organization ensure that third-party providers of information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance, and established service level agreements? AR 25-2, Para. 4-3a(7); DoDI 8500.2 IA Control DCDS			
Are all unit users registered in ATCTS?			
Are all users/user accounts/profiles listed under 32AAMDC Correctly?			
REMARKS:			

Performance Measures	Go	No-Go	N/A
Does the organization review for and verify dormant user accounts (i.e. remove departing users' accounts prior to departure, or terminating accounts which are verified inactive more than 45 days)? AR 25-2, Para. 3-3a(10); Army Password Standards BBP; DoD 8500.2 IA Controls IAAC and IAIA			
Does the organization enforce separation of duties, role-based access, and least privilege through assigned access authorizations for user accounts? AR 25-2, Para. 4-5c; DoDI 8500.2 IA Control ECAN, ECLP, and IAIA			

Are desktops properly configured with an Army approved Data-At-Rest (DAR) solution? AR 25-2, Para. 4-5j(6); Data at Rest BBP; OMB Memorandum - M06-16, Subject: Protection of Sensitive Agency Information; DOD CIO PII Memorandum, 18 August 2006; VCSA ALARACT, dated 10 Oct 2006; DoDI 8500.2 IA Control ECCR			
Do all primary and alternate IMO's have a remedy account and receive remedy emails?			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Do IA personnel, responsible for implementing the IAVM process, subscribe to the Army Knowledge Online (AKO) IAVM Community Group List server? IAW AR 25-2, Para. 4-24d			
Are the IASO, IMO Server/Workstation Administrators and/or alternates ensuring the STAMIS systems (any logical system) and standalone systems are being patched and updated as required? AR 25-2 C4-5			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Does the organization have an incident response plan? (NOTE: A tenant organization must have either their own incident response plan or a copy of the response plan developed by the services provider.) IAW AR 25-2, Para 4-21c; DoDI 8500.2 IA Control VIIR			
Does the incident response plan identify the responsible CND provider? IAW AR 25-2, Para.4-21c; DoDI 8500.2 IA Control VIIR; CJSCM 6510.01A			
Does the incident response plan define reportable incidents? IAW AR 25-2, Para4-21c; DoDI 8500.2 IA Control VIIR; CJCSM 6510.01A			

Does the indicent response plan address response to INFOCON measures? IAW AR 25-2, Para. 4-21c; DoDI 8500.2 IA Control VIIR; CJCSM 6510.01A; STRATCOM Directive 527-1 Para.3.7.5			
Is the incident response plan tested, reviewed, and updated at least annually (or every six months for MAC-I systems)? IAW AR 25-2, Para. 4-21b; DoDI 8500.2 IA Control VIIR			
Are users aware of their responsibility to cease all activity on a computer when they observe suspected security incidents or suspicious IS operation and report immediately to the System Administrator (SA), Information Assurance Manager (IAM), or the Information Assurance Security Officer (IASO)? IAW AR 25-2, Para. 3-3c(9), 4-22a through c			
Does the incident response plan define conditions which require the generation of a Serious Incident Report (SIR)? AR 25-2, Para. 4-21d; DoDI 8500.2 IA Control VIIR			
Do personnel report information system security incidents as required? AR 25-2, Para. 3-2d(3), f(13), and 3-3a(14)			
Does the incident response plan include procedures to isolate the compromised system; and preserve forensic evidence and chain of custody? AR 25-2, Para. 4-22c and d; DoDI 8500.2 IA Control VIIR			
Does the incident response plan include the recovery actions required prior to placing a compromised system back on the network? AR 25-2, Para. 4-23a			
Does the organization understand the requirement to report and respond to classified information spillage events? AR 25-2, Para. 4-21c(8) and d(3); BBP 03-VI-O-0001 (Classified Information Spillage), Para. 11			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Is there an IT contingency plan in place for each Army Information System (IS--A single IS or LAN) as appropriate for essential functions and critical assets identified by the Commander? AR 25-2, Para. 4-5i, DA PAM 25-1-2, Para.2-5a(2); DoDI 8500.2 IA Controls CODP CAT II and COEF CAT II. COMS, COSP			

Has the organization tested all of their IT Contingency Plans (to include training of roles and responsibilities) in the past year (MAC-II or MAC-III); or within the past six months (MAC-I)? AR 25-2. Chap 4-5i; DoDI 8500.2, Section E4.A1; DA PAM 25-1-2, Para. 2e(2), 2-4e(5)a, and 3-4e; AR 500-3, Para. 1-4f and 2-10a; DoDI 8500.2 IA Controls COED-1, COTR, and PRTN			
Does the organization adequately provide physical and technical protection for backup and restoration assets to include backup copies of the operating system and other critical software (to include router tables, configuration settings, and security-related software)? AR 25-2, Para. 4-5i; DoDI 8500.2 IA Control COBR and COSW			
Has the organization documented and tested the necessary system/data recovery procedures? DODI 8500.2 IA Controls COTR-1, COPS, COMS, COSP			
Is the IT Contingency Plan incorporated in the Commander's Continuity of Operations Plan (COOP)? IAW AR 25-1, Para. 6-5			
REMARKS:			

Performance Measures	Go	No-Go	N/A
Is the Army Information Assurance Program actively being implemented in your organization? AR 25-2, Para. 2-24a, f and i			
Are you aware that AR 25-2 and IA Best Business Practices (BBP) are the Army's Information Assurance policies? AR 25-2, Para. 2-24			
Do you know your Information Assurance professionals on your Staff, are they appointed, and are you aware of their roles and responsibilities as delineated in Army Regulation 25-2? AR 25-2, Para. 2-24f, 3-2 and 3-3; DoDI 8500.2 Para E3.4.6			

Do you ensure annual user IA refresher training is conducted and documented? AR 25-2, Para. 4-3a(8)(b); CJCSM 6510.01 Appendix A Enclosure A, 3b(20) and Appendix B Enclosure A Para. 2h and Para. 5; DoD 8570.1-M paragraph C1.4.4.3, C6.2.3, C8.2.7.6; DODD 8570.1 5.9.2			
Do you conduct periodic assessments of your local Information Assurance Program? ALARACT 186/2008			
Are you aware of what Personally Identifiable Information (PII) is and the requirements for protecting PII? ALARACT 167/2007, VCSA SENDS: PII Incident Reporting and Notification Procedures, July 2007; DOD CIO Memorandum, 18 August 2006, Subject: DOD Guidance on Protecting PII; DoDD 5400.11, DoD Privacy Program, Nov 16, 2004			
Do you ensure that FOUO or FOIA information or information not for the public at large has been removed from the organization's official publicly accessible website? AR 25-1, Para. 1-7b; DoD Web Site Admin Policy, Part II, Section 3.5.3; AR 25-2, Para. 4-20g(11), (15), and 3-3i; DoD 5400.7-R, Chapter 3, Section 2.1			
Are you aware of the stringent Information Assurance requirements for protecting wireless networks and systems? AR 25-2 Para 4-29.a.and b.; Wireless Security Standards BBP Para 8.C. and 11.A.(1)			
Are you aware of the procedures to minimize the risks associated with the loss or compromise of sensitive information stored on removable media such as disks and thumb drives? AR 25-2, 4-11(a)(d); AR 25-2, Para. 4-29; DoDI 8500.2 IA Control ECSC; Data-At-Rest (DAR) Protection BBP, Para. 8-E; appropriate DISA STIGS and/or NSA SNAC Guides			
Performance Measures	**Go**	**No-Go**	N/A
Are all Portable Electronic Devices (PEDs) used and procured by the organization on the Army IA Approved Tools List? AR 25-2, Para. 4-29a-f; DoDI 8500.2 IA Control DCAS			
Does the organization configure passwords for Portable Electronic Devices (e.g. Blackberry, Apriva, etc) in accordance with applicable security guides (i.e. DISA STIGs)? DISA Wireless STIG (with appropriate wireless checklist); DoDI 8500.2 IA Control IAIA			

Are unused/unauthorized wireless capabilities (e.g. Bluetooth voice profiles, built-in wireless capabilities of classified devices, etc.) of PEDs disabled prior to issue to end users? Memorandum, CIO/G-6, 1 Aug 06, subject: "Updated Guidance on the Management of BlackBerry Devices with Internal Bluetooth Capability"; DoDI 8500.2 IA Control ECWN			
Does the organization configure portable devices (e.g., Blackberry, Apriva, etc.) in accordance with applicable security guides (i.e., DISA STIGs or NSA guides)? AR 25-2, Para. 4-29; DoDI 8500.2 IA Control ECSC; appropriate DISA STIGS and/or NSA SNAC Guides; Wireless BBP; ALARACT 134/2008			
Are mobile devices (including laptop PCs) properly configured with an Army approved Data-At-Rest (DAR) solution? AR 25-2, Para. 4-5j(6); Data at Rest BBP; OMB Memorandum - M06-16, Subject: Protection of Sensitive Agency Information; DOD CIO PII Memorandum, 18 August 2006; VCSA ALARACT, dated 10 Oct 2006; ALARACT 134/2008; DoDI 8500.2 IA Control ECCR			
Have all users of PEDs received security awareness and user responsibility training to include DAR protection? AR 25-2, Para. 4-29d; BBP 06-EC-O-0008: Data-At-Rest (DAR) Protection, Para. 8-B			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Is there a DD Form 2930 (Privacy Impact Assessment) for each system where electronic Personally Identifiable Information is collected, stored and disseminated by the organization? DA Memo: Subj: Updated Guidance for Submission of Privacy Impact Assessment (s) (PIA), 31 July 2009 (Para 4); DOD Memorandum, Subject: DOD Guidance on Protecting PII, 18 Aug 06 (Para: 4.2 & E2.4.1); DoDI 5400.16 Privacy Impact Assessment (PIA) Guidance, 12 Feb 09; DD Form 2930, Nov 08			

Did the organization assess the likely risk of harm and the relative likelihood of the risk occurring (risk level) caused by the loss or unauthorized disclosure of PII? DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII 05 Jun 09 (Part I b pg 2 & Table 1 Appx A); DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII 18 Aug 06 (Para 4.1)			
Did the organization assign impact categories of High (500+ PII records) or Moderate (Below 500 records)? ALARACT 050/2009, PII Incident Reporting and Notification Procedures (Para 4.3); DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII 05 Jun 09 (Part IV, Pg 9); DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII 18 Aug 06 (Para:4.2)			
Does the organization have written internal command procedures for incident reporting and notification when PII is lost, stolen, or otherwise disclosed to individuals without a duty related, official need to know? ALARACT 050/2009, PII Incident Reporting and Notification Procedures (Para 4.3); DoD Memorandum, Subject: Safeguarding Against and Responding to the Breach of PII 05 Jun 09 (Part IV, Pg 9); DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII 18 Aug 06 (Para:4.3)			
Are mobile computing devices or portable media containing High Impact electronic records that are removed from the protected government workplace signed in and out with a supervising official designated in writing by the security official? DOD CIO Memorandum, Subject: DOD Guidance on Protecting PII, 18Aug06 (Para: 4.2.3.1 & 5)			
REMARKS:			

Performance Measures	Go	No-Go	N/A
Do all Soldiers, DA Civilians, eligible contractors, and foreign national employees who require logical access to the NIPRNET have a Common Access Card (CAC) with identity, signature, and encryption certificates? Army CIO/G-6 ALARACT Army Accelerated Implementation of Common Access Card Cryptographic Network Logon, Para 5.1.2.; JTF-GNO Communication Task Order 06-02, Para 6A.; DoDI 8500.2 IA Control IAKM			

Are all System Administrators using an Alternative Smart Card Logon (ASCL) Token to access their higher privileged account? Army CIO/G-6 Memorandum, Subject: Alternative Smart Card Logon (ASCL) Token for Two-Factor Authentication, Para. 2 and 3; DoDI 8500.2 IA Control ECLP and IAKM			
Are all non-Windows based systems configured for login / authentication using CAC / PKI (or have an approved Army CIO/G-6 waiver)? AR 25-1, Para. 6-5			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Has the organization completed the JBLM NEC Unit OIP Self Assessment Checklist and developed POA&M's to address identified weaknesses and shortcomings at least annually or upon change of the organizations Information Assurance Manager?			
Has the organization completed the CIO G-6 IA Self Assessment Checklist and developed POA&M's to address identified weaknesses and shortcomings at least annually or upon change of the organizations Information Assurance Manager?			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Have the Commander, the Public Affairs Officer (PAO), the OPSEC Officer, and the Webmaster properly cleared information posted to the WWW or to the AKO in areas accessible to all account types? AR 25-1, Para. 6-7a(11); AR 25-2, Para. 4-20g(11), (15), and 3-3i; AR 530-1, Para. 2-3a(15); DoD Web Site Admin Policy, Part I, Para. 5.5.4, 5.5.5, and 5.5.7			

Have all personnel appointed as OPSEC Officers, Webmasters, reviewers (to include PAO), and content managers received OPSEC web content vulnerability and web risk assessment training? AR 530-1, Para. 4-3b(2); DA Pam 25-1-1, Para. 8-4b			
Has FOUO, FOIA-exempt, or other non-public information been removed from a unit's publicly accessible website? AR 25-1, Para. 1-7b and 6-7c(4); AR 530-1, Para. 2-3a(15a); DoD Web Site Admin Policy, Part II, Section 3.5.3; DoD 5400.7-R, Para. C3.2			
Are publicly accessible websites behind an Army Reverse Proxy Server? AR 25-2, Para. 4-20g(12); AR 25-1, Para. 6-7c(6a)			
Is this publicly accessible website hosted on the ".mil" domain? DA Pam 25-1-1, Para. 8-1d; AR 25-1, Para. 6-4n(11); Office of Management and Budget (OMB) Memorandum dated 17 DEC 2004, Para. 6a.			
Are the unit's publicly accessible telephone directories generic? (Such as no names or personally identifying information.) AR 25-1, Para. 6-4 r(1)			
Does the organization ensure their public web site(s) are registered and posted on the Army "A-Z" page (www.army.mil/A-Z)? DA Pam 25-1-1, Para. 8-1e			
Have all private (non-public) web sites been configured to require, at a minimum, Class 3 DoD PKI certificates for identification and authentication? AR 25-2 Para. 4-20 g(14); ALARACT 180/2006, Para. 4A1& 4B; DoDI 8500.2 IA Control IATS			
REMARKS:			
Performance Measures	**Go**	**No-Go**	**N/A**
Are unauthorized wireless devices (WLAN, RF keyboards, RF mice, Bluetooth devices, etc) immediately removed/shut down and reported to the DOIM/NEC/RCERT? IAW AR 25-2, 4-22 and 4-30a; Army Wireless Security Standards BBP Para. 5A(4); DoDI 8500.2 IA Control ECWN			

Are wireless NICs logically (Unclassified systems only) or physically (Classified or Unclassified systems) disabled on computer systems/PEDs connected to a wired network? DODD 8100.02 Para. 4.7; DoDI 8500.2 IA Control ECWN			
Are approved wireless IA devices/tools used to secure approved / accredited wireless LAN devices / architectures? AR 25-2, Para. 4-1.d and 4-5l; Army Wireless Security Standards BBP, Para. 7; IA Tools BBP, Para. 4, 10, and 11; DoDI 8500.2 IA Control DCAS and ECWN			
Are approved encryption mechanisms in place for all approved / accredited WLAN devices connected to the installation network(s)? AR 25-2, Para. 6-1; DoDD 8100.2, Para. 4.1.2. through 4.1.3; Army Wireless Security Standards BBP, Para 5F; DoDI 8500.2 IA Control ECCT			
REMARKS:			